Single Connect Kron

Datasheet

PROTECT WHAT YOU CONNECT™

In today's digital world, there are many cyber security threats such as trojan, ransomware, malware, phishing, social media attacks and many more. **World Economic Forum (WEF) indicates in its "The Global Risks Report 2020" that infrastructure and money/data theft related cyberattacks will be increased at least 75% in 2020.**

Also, Grand Theft Data from McAfee reports internal actors were involved in 43% of data breaches, half intentional and half unintentional. **Human, is probably the weakest link in cyber security and privileged accounts** (local admin accounts, privileged user accounts, domain administrative accounts, etc.) are the top priority of all, which must be monitored and controlled closely by carriers and enterprises.

PAM security solutions enforce privilege access controls, **minimizing shared, credential risk while controlling applications and endpoint devices (servers, routers, etc.).** Unlike IAM (Identity and Access Management), which permits consumers and other outsiders to access a company's applications, websites, and databases, PAM (Privileged Access Management) focuses on controlling and securing the internal IT environment of an organization.

Single Connect, as a PAM solution, supports wide range of features in one box and helps carriers/enterprises to establish a flexible, centrally managed and layered defense security architecture against insider threats.

Unified Management of Privileged Access Accounts

Kron Single Connect product family strengthens, **simplifies and secures the management of privileged accounts**, for enterprises and network operators who serve them. Single Connect unifies multivendor environments with pre-integrated modules managing dozens of vendors and hundreds of network elements and servers with a single, universal system.

Single Connect product family enables IT & network administrators to:

- Efficiently secure access to network infrastructure and applications
- Transparently enforce company security policies on privileged sessions
- Conveniently and universally control configurations
- Comprehensively record all activities in the network and data center that impact business continuity

Single Connect Kron

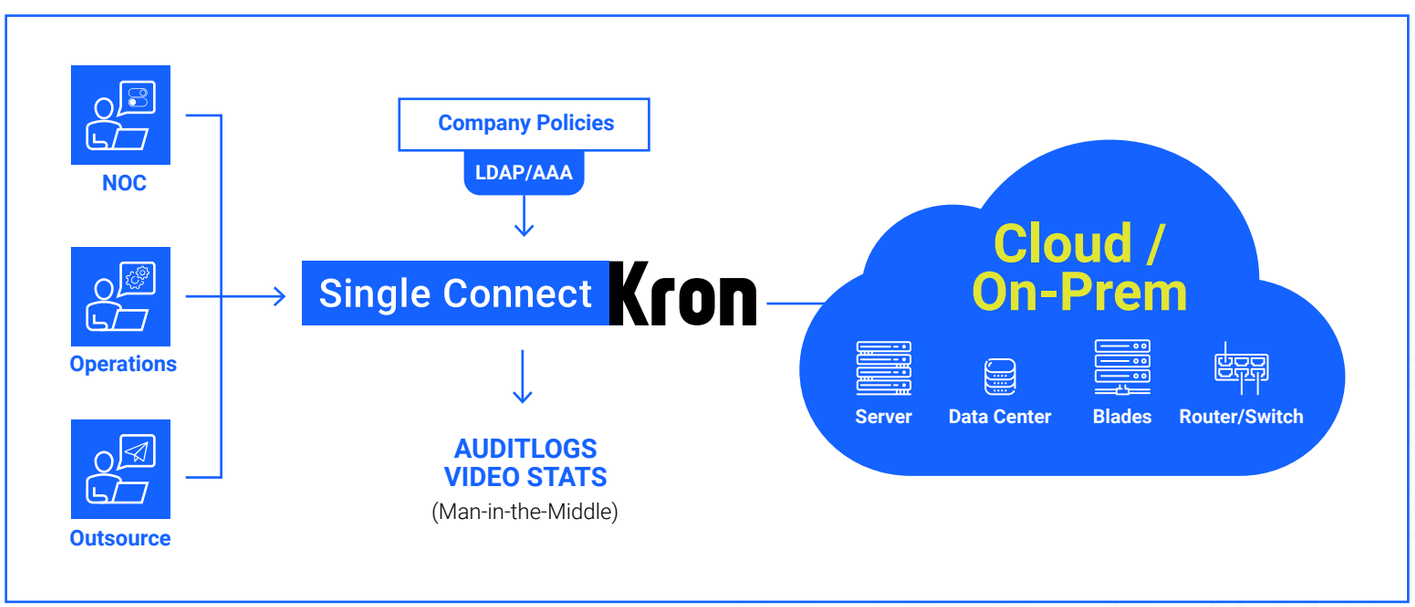
Datasheet

STRONGER, SIMPLER AND MORE SECURE

Cloud-native and designed to support Software Defined Networks today and in the future, Single Connect prevents and detects breaches, maintains individual accountability and increases operational efficiency significantly by managing credentials and delegating privileged actions.

This proven solution reduces implementation time required to set up privileged access control by approximately 80% compared to other solutions and can scale to support tens of thousands of users and accounts, millions of devices and endpoints, and billions of authentication combinations.

Whether applied to real time communications systems, desktops, mobile devices and collaboration applications, or to connected machines as part of Internet of Things deployments, Single Connect dramatically reduces the complexity associated with a fully effective, fully compliant solution.



Single Connect™ basically provides a solution for the following risks and obligations

- Internal & External Security Breaches
- Many Faulty Engineering Actions
- Controlling of Multi-Vendor Support & Maintenance services
- Malware that targets privileged accounts
- Governance Requirement of Regulatory Bodies (GDPR, PCI DSS, ISO 27002 etc.)

Single Connect Kron

Datasheet

PRODUCT FAMILY

Dynamic Password Controller

Takes control of device and database passwords, providing security while sustaining efficiency.

Unified Access Manager

Provides AAA services for network infrastructure and extends authentication and policy configurations of AD to network.

Privileged Session Manager

Logging and recording of all sessions for network and servers, including command and context-aware filtering.

Database Access Manager

Single point of access control management for database layer, secures data access with logging, policy enforcement, and masking.

Two-Factor Authentication

Additional layers of authentication integrating mobile device, geo-location and time.

Privileged Task Automation

Provided a single interface to configure the ability of network business flows with dynamic and extendable command sets.

Dynamic Password Controller

Single Connect Dynamic Password Controller is a central secure password vault and helps to prevent stealing or unauthorized sharing of passwords. Users check-out the credentials of a privileged account from Single Connect Dynamic Password Controller and then uses the password to connect to target endpoint in order to fulfil their tasks. Indexed logging and audit trail is generated to meet the security and compliance requirements. Dynamic Password Controller supports integration with the existing directory service of enterprises so that users continue to use their existing personal accounts to login to Single Connect Dynamic Password Controller and check-out the credentials of the target privileged accounts they are authorized to. Dynamic Password Controller secures the user credentials of operating systems (Windows, Linux, Unix), databases (Oracle, MySQL, MsSQL, PostgreSQL, etc.), virtually any network device or appliance that has an SSH/TELNET interface and any application that provides user credential management API's.

Application-to-Application Password Management (AAPM) to eliminate static passwords in configuration files and source codes of application is supported with agentless architecture.
Secret Vault enables secure storing, tracking and sharing of confidential data/file or unmanaged credentials among employees.

Single Connect Kron

Datasheet

Privileged Session Manager

Single Connect Privileged Session Manager (PSM) has the capability to control, monitor and audit encrypted administrator sessions. Session manager runs as a gateway between users and target end points. **Man-in-the-middle approach** of Privileged Session Manager requires no software agents **to be deployed** to target end points and also no specific access portal or **client application is required** to go through. It is fast to implement and has no impact on end-user experience. Users are authenticated from the existing directory service of the enterprise, and the entire session goes through Privileged Session Manager therefore indexed logs, audit trails, videos and statistics are generated indisputably. Any custom policy can be created flexibly on **Privileged Session** Manager and can be assigned to user groups to implement the least privilege practices within the enterprise. Single Connect Privileged Session Manager supports a wide range of interfaces including **SSH/TELNET** for command line interface sessions, RDP/VNC for remote desktop connections, HTTP(S) for web sessions, SFTP for file transfers.

Two-Factor Authentication (2FA) Manager

Usernames and passwords were the most common **combination** to identify users, but today passwords are vulnerable and hackers may easily steal passwords with phishing, social or dictionary attacks. **2FA Manager** delivers an additional code (one-time-password) to mobile phones of users that is required to be entered during authentication which assures users are who they say they are. **2FA Manager** can work with any application or device that supports RADIUS Access-Challenge mechanism. 2FA Manager supports integration with the existing directory service of enterprises so that users continue to use their existing personal accounts. One time password can be delivered to users in real-time through **Single Connect Mobile application or SMS**. Offline code generation is also supported through Single Connect Mobile application and key generator hard tokens.

Unified Access Manager

Controlling access to who can login to a network device or server via **SSH/TELNET** sessions to configure them has always been a high priority concerns for carriers and enterprises. Longstanding de-facto protocols for device administration access management are RADIUS (Remote Access Dial-in Service) and TACACS (Terminal Access Controller Access-Control System). Every authentication and command execution attempt of a user is forwarded from device/server to Single Connect **TACACS** Manager which enables many features –including single-sign-on, custom/least policy enforcement, indisputably logging, multi-tenancy) to be centrally managed and delivered.

Database Access Manager

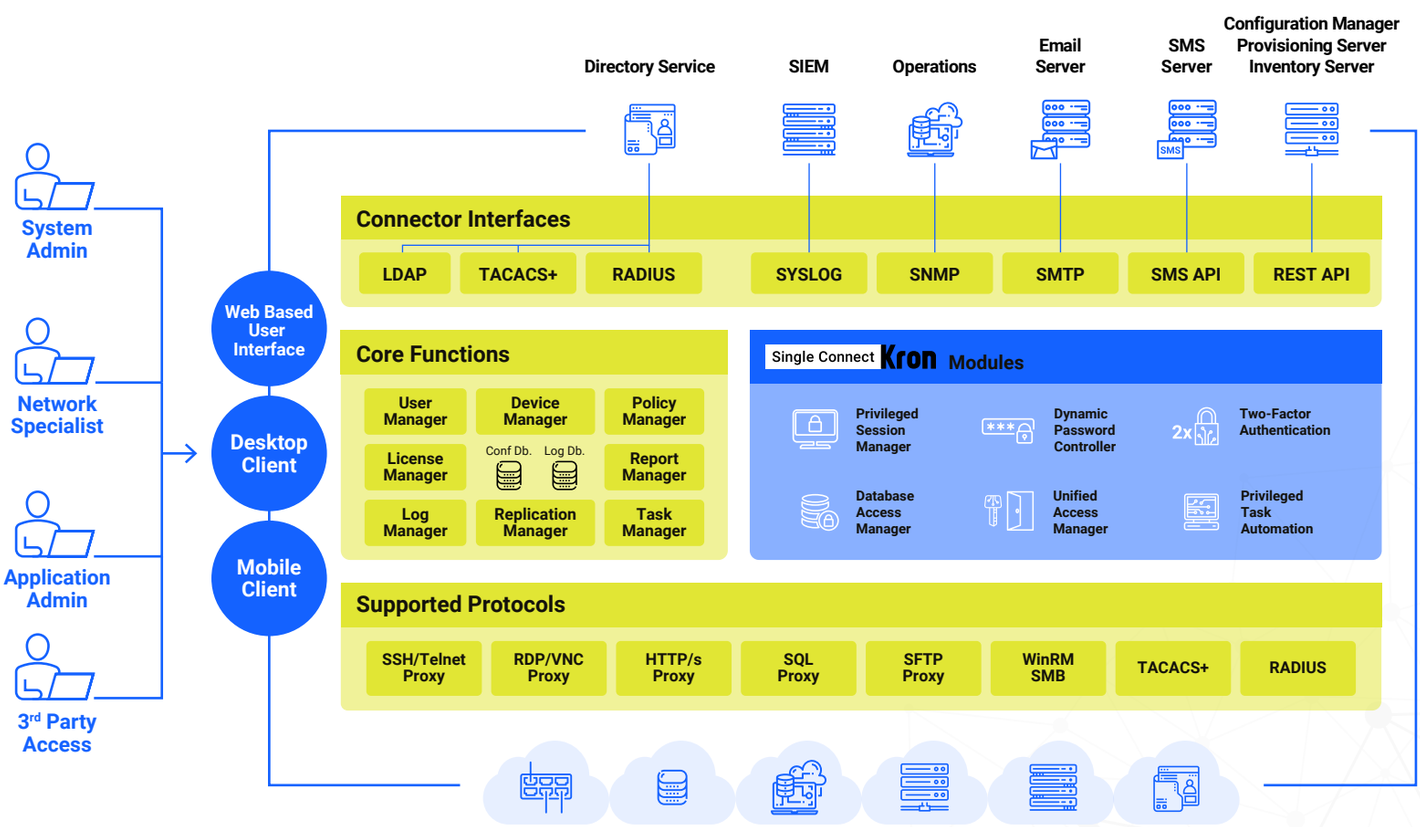
Single Connect Database Access Manager has the capability to control, monitor and audit encrypted database administrator sessions. Database Access Manager **runs as a gateway** between users and target databases. Man-in-the-middle approach of **Database Access Manager** requires no software agents to be deployed to target end points and no specific access portal or client application is required to go through. It is fast to implement and has no impact on end-user experience. Users are **authenticated** from the existing directory service of the enterprise, and the entire session goes through Database Access Manager therefore indexed logs, audit trails and statistics are generated indisputably. Any custom policy can be created flexibly on Database Access Manager and can be assigned to user groups to implement the least privilege practices within the enterprise. Single Connect Privileged Session Manager supports a wide range of **SQL** and **NoSQL** database types for DB sessions including Oracle, MsSQL, **MySQL**, Cassandra, Teradata and Hive. Single Connect Database Access Manager efficient and centrally secures and controls privileged access to databases. Single Connect Database Access Manager also provides dynamic data masking feature to **prevent access** to sensitive data.

Single Connect Kron

Datasheet

HOW IT WORKS

Single Connect has modular and integrated architecture to support wide range of protocols and features on one platform.



Endpoints: Servers, devices, applications, databases, fileservers, appliances etc.

Users logon to Single Connect from web based interface to use services such as web based remote desktop connection to a windows server, web based CLI connection to a network device, password checkout from secure vault, etc.

Users may prefer to connect using their regular native clients instead of web based interface. For example, users can use their own CLI client applications (e.g. Putty, SecureCRT) or Windows native remote desktop application or SQL client (TOAD, DataGrid, Navicat, etc.) applications to connect directly to Single Connect proxy services which are SSH/TELNET, RDP and SQL respectively in this case.

In some use cases, users do not directly connect to Single connect or even aware of Single Connect. For example, if a network device is managed by Single Connect Unified Access Manager, when a user directly connects to that device for administration purposes, Single Connect runs behind the scenes and user is not even aware of Single Connect.

Single Connect admins connect via Web based interface for administration and configuration purposes such as changing user privileges, creating new policies, adding/removing endpoints and monitoring user sessions.

Single Connect Kron

Datasheet

BUSINESS BENEFITS

Full visibility and **full control** are achieved without compromising **operational** efficiency	Integrated User Behavior (**UBA**) Analytics & OCR	**Modular** - Ready to add modules for your future needs
Enforce Security Policies Transparently	**Network Automation** for Security - Automation increases security while maintaining organizational agility	**Fastest to deploy** - Fastest to deploy PAM available in the market
Manage and **Record** Every Users Activity	**Centralized** - Unified visibility and management of all privileged sessions	**After-the-Fact Records** - Indisputable indexed logging and session recording
Isolation of **critical target systems** from user network	**Agent-less** - No agent software on endpoints.	**Least Privilege** - Best-in-class Real-Time Least Privilege Management
Segregation of Duties & Least privilege functions including command or application-based restrictions, managerial approval, geo-location confirmation, time & date-based access	**Seamless** - Admins continue to use their native client apps	**Accountability** - Enables accountability and records for investigations
	Transparent - Enforces Security Policies transparently	**Password Management** - Eliminates password sharing and strengthens credentials
Enforce role-base **access controls** centrally and silently	**Real-Time Prevention** - Prevent malicious activities before they occur	**Security** - Securely stores passwords in vault
Shared Account Password Management	**Comprehensive** - Industry's widest support range for protocols	**Protocols** - Industry's widest support range for protocols
Compliancy with **regulations**, Internal Operations **Auditing** and **Screening**	**Scalable** - Supports tens of thousands of endpoints with a standard server	**Cloud** - Supports Cloud platforms